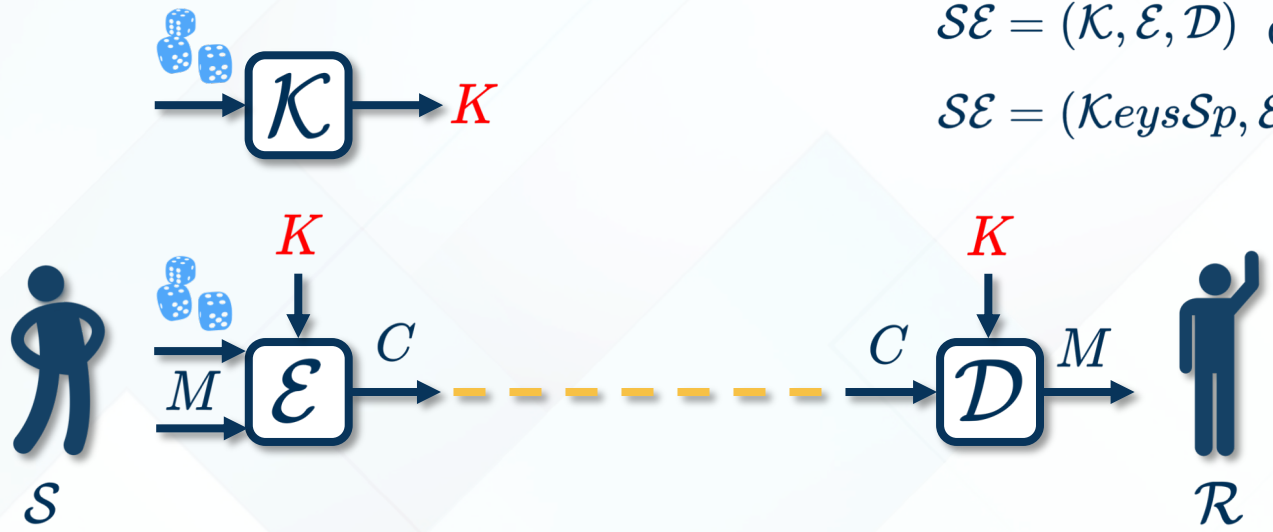
SYMMETRIC ENCRYPTION
ENCRYPTION MODES
SECURITY NOTIONS

- A scheme $\mathcal{SE}$ is specified by 3 algorithms $\mathcal{K}$ (or $\mathcal{KeySp}$), $\mathcal{E}$, $\mathcal{D}$ and the message space $\mathcal{MsgSp}$.

$$\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D}) \text{ or}$$

$$\mathcal{SE} = (\mathcal{KeysSp}, \mathcal{E}, \mathcal{D})$$

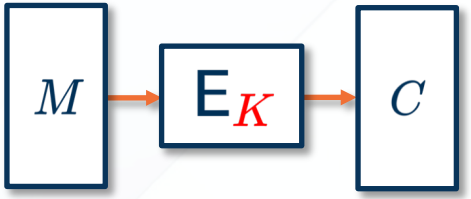


It is required that for every $M \in \mathcal{MsgSp}$ and every $K \in \mathcal{KeySp}$ (or output by $\mathcal{K}$), $\mathcal{D}(K, \mathcal{E}(K, M)) = M$.

- Often the key generation algorithm simply picks a random string from some key space $\mathcal{KeySp}$ (e.g. $\{0,1\}^k$ for some integer k) .
  - In this case we will say that a scheme $\mathcal{SE}$ is defined by $\mathcal{KeySp}$ and two algorithms: $\mathcal{SE} = (\mathcal{KeySp}, \mathcal{E}, \mathcal{D})$
- The encryption algorithm can be
  - randomized (take as input a random string)
  - stateful (take as input some state (e.g. counter) that it can update)

Blockciphers, the main tool of symmetric crypto

- Examples: DES, 3DES, AES…
  - A tool to encrypt short strings
  - A block cipher is a function family $\mathsf{E} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, where k (key length), n (input and output lengths) are the parameters



  - Notation: for every $K \in \{0,1\}^k, \mathsf{E}_K : \mathsf{E}(K, M)$
  - For every $K \in \{0,1\}^k$, $\mathsf{E}_K(\cdot)$ is a permutation (one-to-one and onto function) on $\{0,1\}^n$

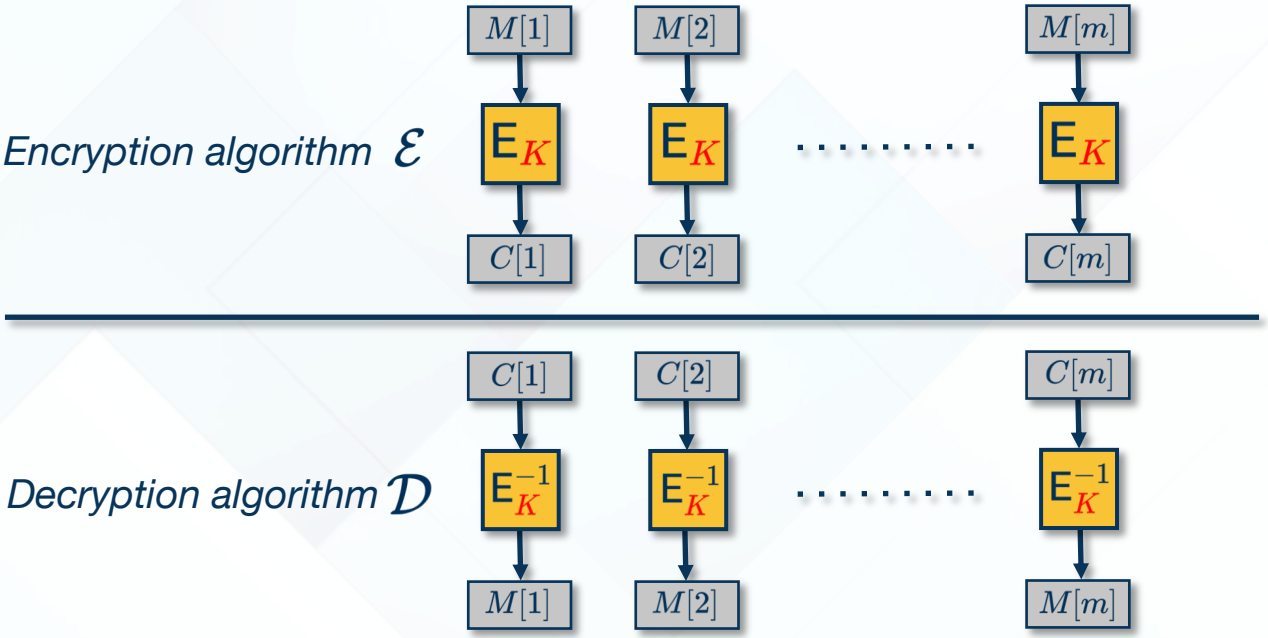
    For every $C \in \{0,1\}^n$ there is a single $M \in \{0,1\}^n$ s.t. $C = \mathsf{E}_K(M)$
  - Each blockcipher has an inverse denoted $\mathsf{E}_K^{-1}(\cdot)$ s.t. $\mathsf{E}_K(\mathsf{E}_K^{-1}(C)) = C, \mathsf{E}_K^{-1}(\mathsf{E}_K(M)) = M$ for all $M, C \in \{0,1\}^n$

Blockcipher modes of operation

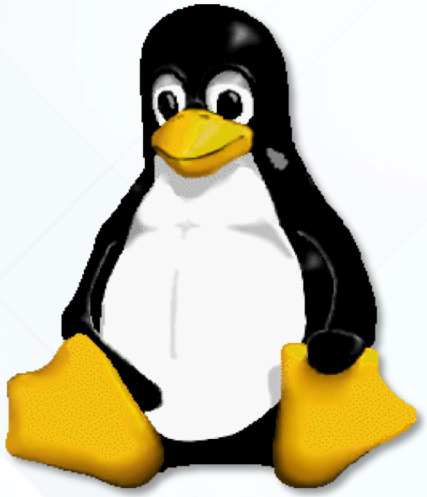
- Modes of operation define how to use a block cipher to encrypt long messages
- For simplicity we will often assume that the message space consists of messages whose length is multiple of a block length (otherwise, messages can be padded)

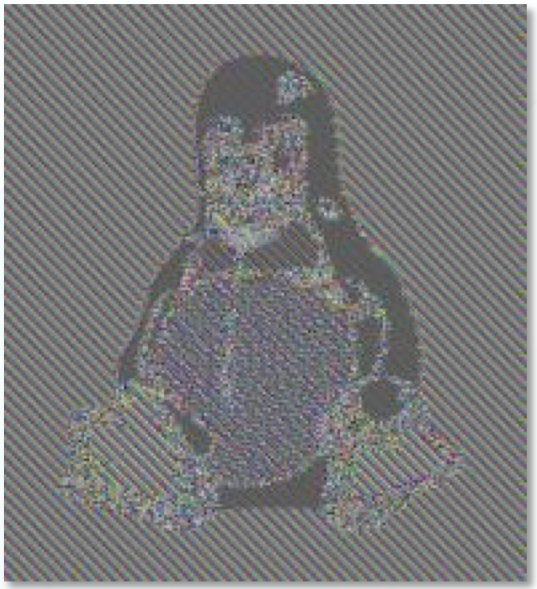
Electronic Code Book (ECB) mode

- Let $\mathsf{E} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. $\mathrm{ECB} = (\{0,1\}^k, \mathcal{E}, \mathcal{D})$:



Encrypt an image with ECB





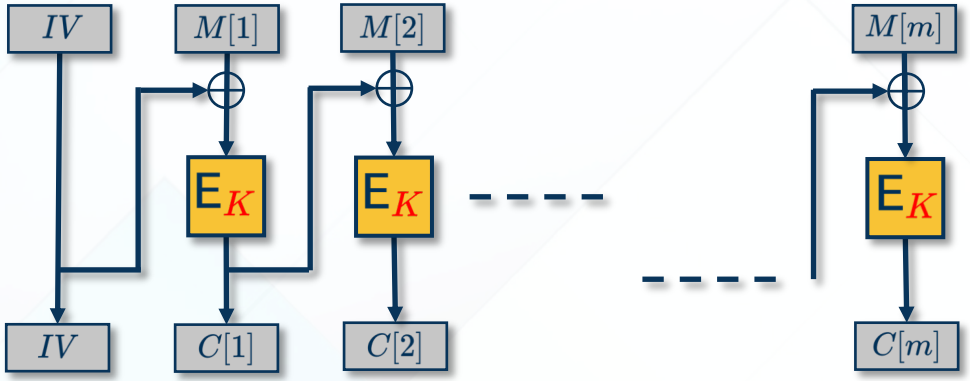
Cipher-block chaining (CBC) mode with random IV

Let $\mathsf{E} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher.

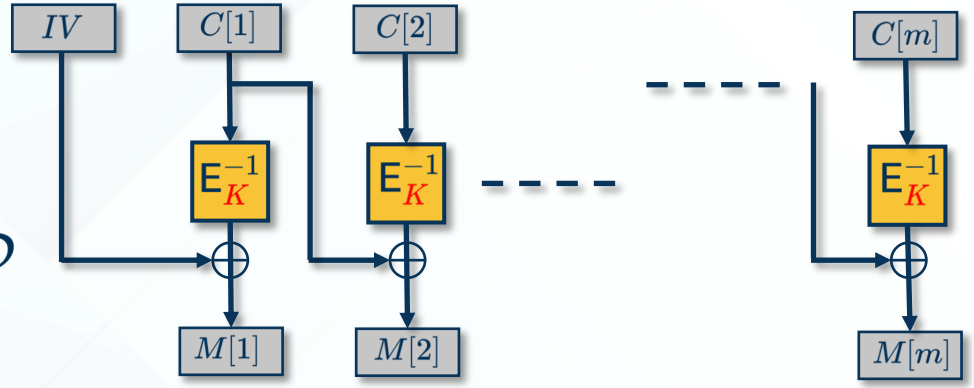
$\mathsf{CBC\$} = (\{0,1\}^k, \mathcal{E}, \mathcal{D})$:

Encryption algorithm $\mathcal{E}$

$IV \xleftarrow{\$} \{0,1\}^n$



Decryption algorithm $\mathcal{D}$



Georgia Tech

Stateful cipher-block chaining (CBC) mode with counter IV

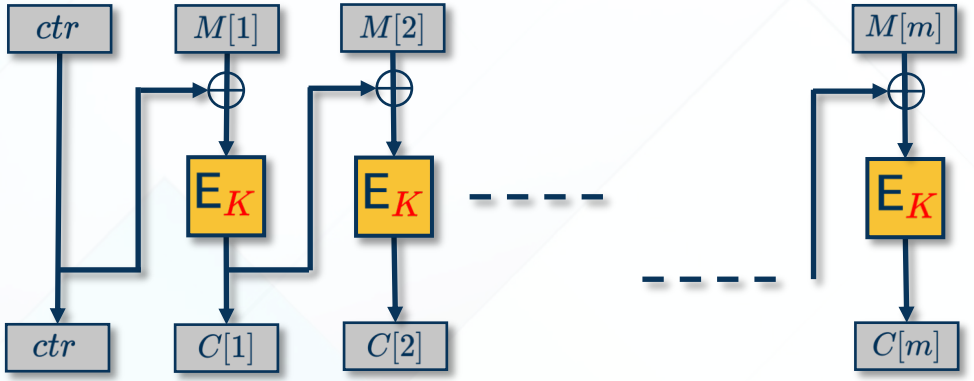
Let E : $\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher.

CBCC $= (\{0,1\}^k, \mathcal{E}, \mathcal{D})$:

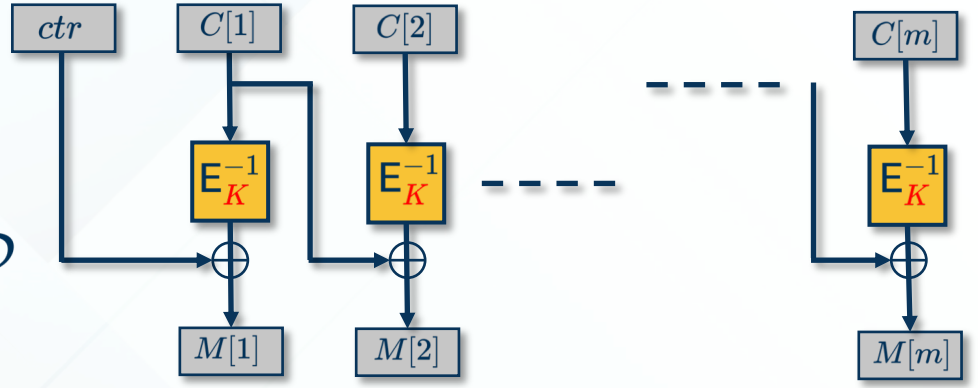
Encryption algorithm $\mathcal{E}$

The counter is incremented for each message until it wraps around

$ctr \leftarrow 0^n$



Decryption algorithm $\mathcal{D}$



Georgia Tech

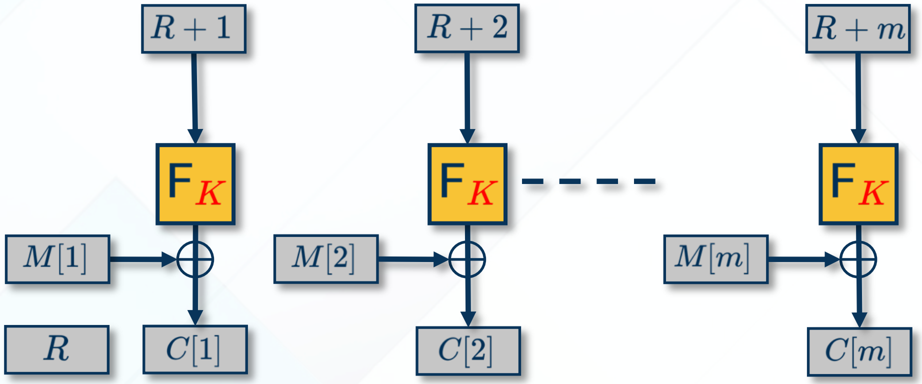
Randomized counter mode (CTR\$)

Let F : $\{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^L$ be a function family.

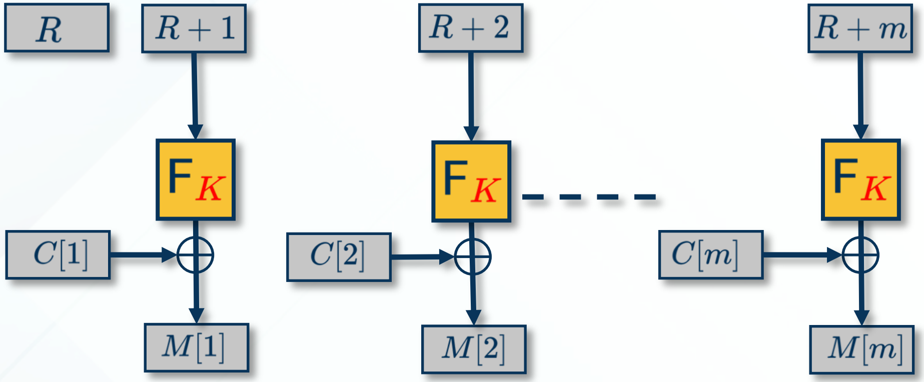
CTR\$ $= (\{0,1\}^k, \mathcal{E}, \mathcal{D})$:

Encryption algorithm $\mathcal{E}$

$$R \xleftarrow{\$} \{0,1\}^l$$



Decryption algorithm $\mathcal{D}$



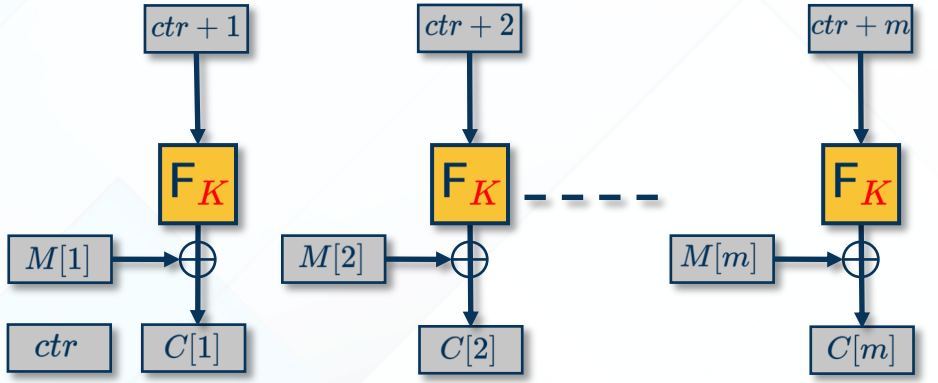
Stateful counter mode (CTRC)

Let $\mathsf{F} : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^L$ be a function family.
$\mathsf{CTRC} = (\{0,1\}^k, \mathcal{E}, \mathcal{D})$:

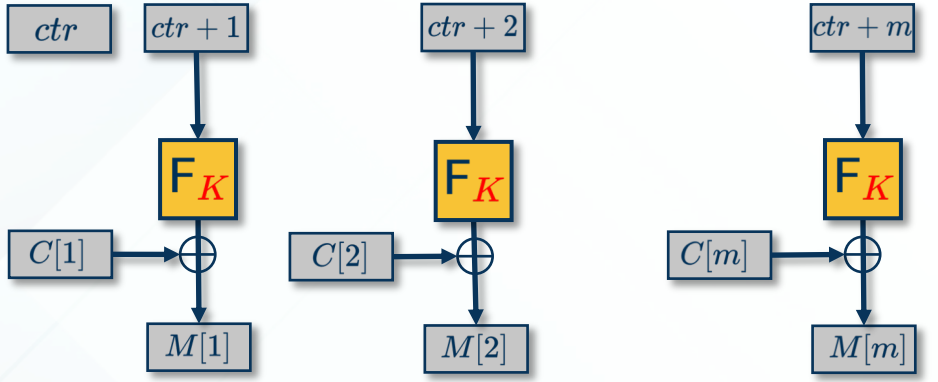
A current counter is ctr maintained as a state

Encryption algorithm $\mathcal{E}$

ctr is initially 0^l



Decryption algorithm $\mathcal{D}$



Georgia Tech

What is a secure encryption scheme?

- Recall, perfectly secure schemes are impractical
- We assume that adversaries are computationally bounded
- A scheme is secure when it is not insecure
- Insecure = adversaries can do bad things
- Bad things: an adversary, who sees ciphertexts
  - can compute the secret key
  - can compute some plaintexts
  - can compute the first bit of a plaintext
  - can compute the sum of the bits of a plaintext
  - can see when equal messages are encrypted
  - can compute …

So what is a secure encryption scheme?

- Informally, an encryption scheme is secure if no adversary with "reasonable" resources who sees several ciphertexts can compute any* partial information about the plaintexts, besides some a-priori information.

  * Any information, except the length of the plaintexts. We assume the length of the plaintexts is public.

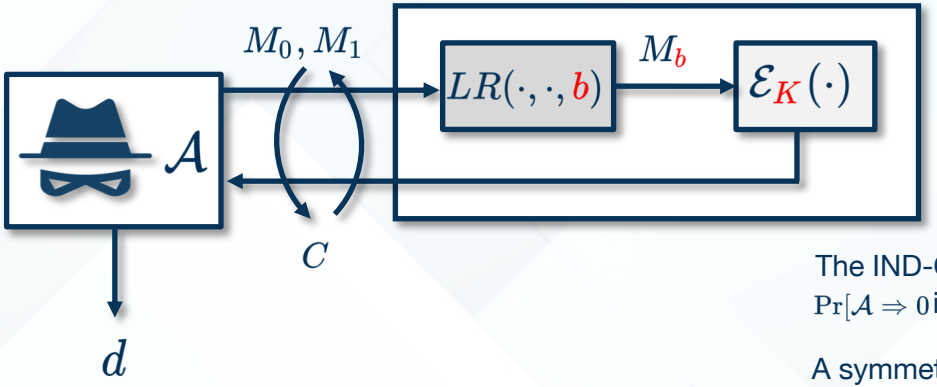
- Note, that the above implies that the bad things we mentioned do not happen. And the other "bad" things.
- While the above "definition" captures the right intuition, it's too informal to be useful.

Indistinguishability under chosen-plaintext attacks

Fix $\mathcal{SE} = (\mathcal{KeySp}, \mathcal{E}, \mathcal{D})$, $K \xleftarrow{\$} \mathcal{KeySp}$

For an adversary $\mathcal{A}$ and a bit b (either 0 or 1) consider an experiment ind-cpa-b, i.e., consider two experiments, ind-cpa-0 (“left”) and ind-cpa-1 (“right”).

In each experiment, $\mathcal{A}$ is given access to the “left-right” encryption oracle that takes two messages and returns encryption of M_b under K



The IND-CPA advantage of $\mathcal{A}$ (denoted as $\mathrm{Adv}^{\text{ind-cpa}}(\mathcal{A})$) is $\Pr[\mathcal{A} \Rightarrow 0 \text{ in ind-cpa-0 exp.}] - \Pr[\mathcal{A} \Rightarrow 0 \text{ in ind-cpa-1 exp.}]$.

A symmetric encryption scheme $\mathcal{SE}$ is indistinguishable under chosen-plaintext attacks (IND-CPA secure) if for any adversary $\mathcal{A}$ with “reasonable” resources its ind-cpa advantage is “small” (close to 0).

Resources of an adversary

1. Time-complexity is measured in some fixed RAM model of computation and includes the maximum of the running-times of $\mathcal{A}$ in the experiments, plus the size of the code for $\mathcal{A}$.
2. The number of queries $\mathcal{A}$ makes.
3. The total length of all queries.

How to prove a scheme is not secure

1. Construct an adversary (present a pseudocode for its algorithm) that breaks the scheme(e.g. ECB) according to the definition of security in question (e.g. IND-CPA).
2. Calculate the adversary's advantage. It shouldn't be too close to 0. E.g. something like $1/2^{60}$ is too small. 1/1000 is OK (for the adversary, not security).
3. Calculate the adversary's resources (time, number of queries, total number of bits in queries). They should be "reasonable". E.g., 2^{60} queries is not reasonable.

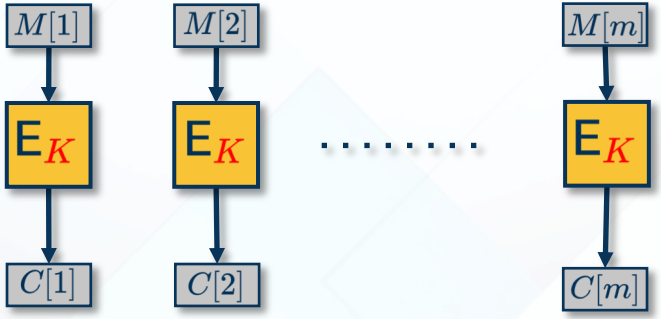
Let’s test IND-CPA definition

- Consider various toy examples.

Analysis of the ECB mode

Let $\mathsf{E} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. $\mathrm{ECB} = (\{0,1\}^k, \mathcal{E}, \mathcal{D})$:

Encryption algorithm $\mathcal{E}$



- Is ECB a good encryption scheme?
- Is ECB IND-CPA secure?

ECB is not IND-CPA

- **Claim**: any deterministic, stateless scheme is not IND-CPA.

- Why?

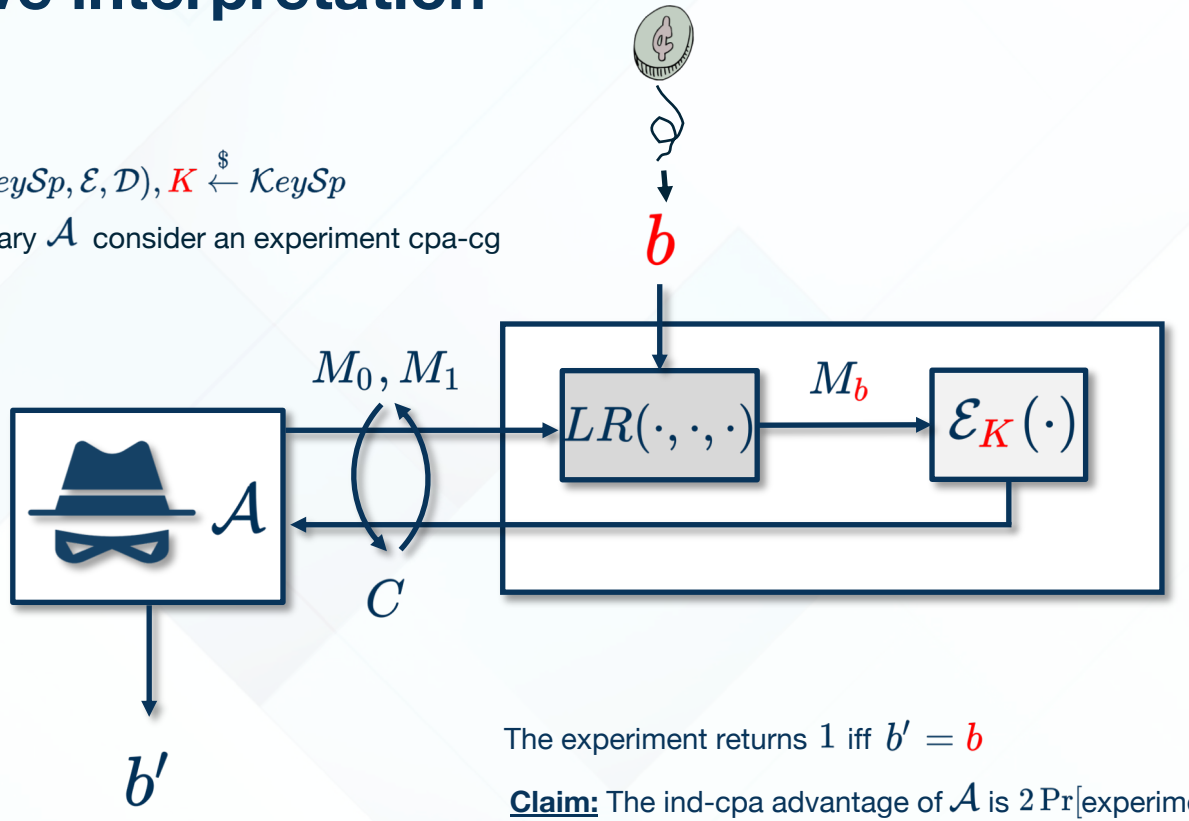
CBCC is not IND-CPA

- Turns out that the rest of the modes are IND-CPA secure assuming that the underlying blockcipher is good.
- Before that we will learn what does it mean for a blockcipher to be good.

Alternative interpretation

Fix $\mathcal{SE} = (\mathcal{KeySp}, \mathcal{E}, \mathcal{D}), K \xleftarrow{\$} \mathcal{KeySp}$

For an adversary $\mathcal{A}$ consider an experiment cpa-cg



The experiment returns 1 iff $b' = b$

Claim: The ind-cpa advantage of $\mathcal{A}$ is $2\Pr[\text{experiment cpa-cg returns } 1] - 1$.

Proof